Blockchain Security Monthly Recap of April: $94.07M lost in attacks

Beosin · Follow
4 min read · 4 days ago

Listen Share

According to Beosin EagleEye, in April 2023, the number of various security incidents and the amount involved decreased compared with March. In this month, more than 19 typical security incidents occurred and the total loss of various security incidents was about $94.07M, which is down about 56.8% compared with March.

The biggest security incident in April was the attacks on several MEV bots, which caused a loss of $25M. In addition, there were two cases of hot wallet theft and the loss of each case was more than $10M. There were several rug pulls of more than $1M. Users need to pay more attention to the potential risks of projects.

DeFi

『9』Typical Security Incidents

№1 On April 2, Allbridge was under a flash loan attack and had a loss of about $550,000.

№2 On April 3, several MEV bots were under sandwich attacks with a total loss of $25 million.

№3 On April 5, Sentiment, a DeFi lending protocol, was attacked and lost about $1,000,000.

№4 On April 9, SushiSwap suffered an attack with a loss of $3.34 million.

№5 On April 10, Terraport was attacked by APT organization, losing about $4 million.

№6 On April 12, MetaPoint was attacked with a loss of about $910,000.

№7 On April 13, Yearn Finance was under a flash loan attack and suffered a loss of $11.5 million.

№8 On April 15, Hundred Finance, an Optimism-based project, was under a flash loan attack with a loss of about $7 million.

№9 On April 28, 0vix Protocol, a Polygon-based project, was attacked with a loss of about $2,000,000.

Exchange

『2』Typical Security Incidents

№1 On April 9, GDAC, a Korean crypto exchange, lost about $13 million because its hot wallet was attacked.

№2 On April 14, the hot wallet of Bitrue was compromised with a loss of about $24 million.

Wallet/User Security

『1』Typical Security Incidents

№1 On April 22, Trust Wallet shared a vulnerability affecting new addresses created Nov 14–23, 22 using the Browser Extension.

Rug Pull/Crypto Scam

『5』Typical Security Incidents

№1 On April 2, Kokomo Finance, an Optimism-based lending protocol, had a rug pull of $1,500,000.

№2 On April 9, CoreHunter, a Zksync project, had a rug pull and the contract deployer made a profit of about $510,000.

№3 On April 13, SyncDex, a Zksync project, had a rug pull and the contract deployer made a profit of about $370,000.

№4 On April 25, Ordinals Finance had a rug pull and the deployer made a profit of $1,010,000.

№5 On April 26, Merlin Dex had a rug pull and the total loss was $1,800,000.

Crypto Crime

『1』Typical Security Incidents

№1 On April 24, The U.S. Treasury Department sanctioned 3 North Koreans for supporting the Lazarus Group, a North Korean hacking team known for crypto thefts.

Others

『1』Typical Security Incidents

№1 In April, phishing scams were showing up frequently at the top of Google Search and caused more than $4 million worth of crypto assets stolen.

In view of the current new situation in the field of blockchain security, Beosin concludes:

Generally, in April 2023, the number of various security incidents and the amount involved decreased compared with March. The total loss of various security incidents was about $94.07M, which is down about 56.8% compared with last month.

The number of rug pulls, however, did not decreased. The number of rug pulls on Zksync even increased. Users are advised to be more careful and conduct a detailed background investigation of projects. The loss of exchange hot wallets in April was tremendous. Exchanges should pay attention to off-chain security and protect their private keys. There were several flash loan attacks with great losses in April. It is recommended that the project teams must take business logic security into consideration during the development and seek a professional security company for audit before launching their projects.

Beosin is a leading global blockchain security company co-founded by several professors from world-renowned universities and there are 40+ PhDs in the team. It has offices in Singapore, Korea, Japan, and other 10+ countries. With the mission of “Securing Blockchain Ecosystem”, Beosin provides “All-in-one” blockchain security solution covering Smart Contract Audit, Risk Monitoring & Alert, KYT/AML, and Crypto Tracing. Beosin has already audited more than 3000 smart contracts and protected more than $500 billion funds of our clients.